Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/CN05/000376

International filing date: 24 March 2005 (24.03.2005)

Document type: Certified copy of priority document

Document details: Country/Office: CN
Number: 200410030517.1
Filing date: 02 April 2004 (02.04.2004)

Date of receipt at the International Bureau: 24 May 2005 (24.05.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

PCT/CN2005/000376

证　　明

本证明之附件是向本局提交的下列专利申请副本

申　请　日：　2004.04.02

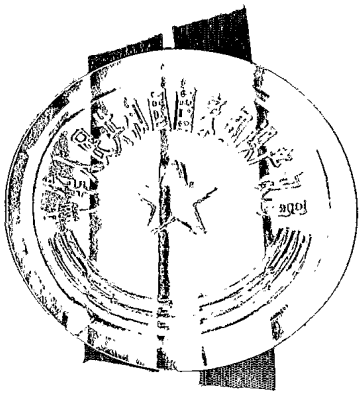
申　请　号：　200410030517.1

申请类别：　发明

发明创造名称：　一种实现漫游用户使用拜访网络内业务的方法

申　请　人：　华为技术有限公司

发明人或设计人：　黄迎新、张文林



中华人民共和国
国家知识产权局局长　王景川

2005 年 4 月 12 日

权 利 要 求 书

1、一种实现漫游用户使用拜访网络内业务的方法，其特征在于，该方法包括以下步骤：

拜访网络内的业务服务器接收到来自漫游用户的包含 TID 信息的业务请求消息后，根据该漫游用户所属归属网络的通用鉴权框架鉴权结果，建立拜访网络内业务服务器和漫游用户之间的信任关系，实现漫游用户使用拜访网络内业务。

2、根据权利要求 1 所述的方法，其特征在于，所述根据该漫游用户所属归属网络的通用鉴权框架的鉴权结果，建立拜访网络业务内服务器和漫游用户之间的信任关系进一步包括以下步骤：

a、拜访网络内的业务服务器直接向本网络内的 BSF 或通用鉴权框架代理发送查询该 TID 所对应的用户是否合法的消息；

b、接收到步骤 a 所述查询消息的 BSF 或通用鉴权框架代理，直接向归属网络内的 BSF 发送查询与该 TID 所对应的用户是否合法的消息；

c、归属网络内的 BSF 在本地检测到与该 TID 对应的用户信息后，给拜访网络内的 BSF 或通用鉴权框架代理返回与该 TID 对应的用户信息；

d、拜访网络内的业务服务器接收到本网络内的 BSF 或通用鉴权框架代理返回的与该 TID 对应的用户信息后，建立与该漫游用户之间的信任关系。

3、根据权利要求 2 所述的方法，其特征在于，所述通用鉴权框架代理是一个独立的服务器，或与本网络内的 AAA 服务器合设的服务器，或与本网络内的业务服务器合设的服务器。

4、根据权利要求 1 所述的方法，其特征在于，所述根据该漫游用户所属归属网络的通用鉴权框架的鉴权结果，建立拜访网络内业务服务器和漫游用户之间的信任关系进一步包括以下步骤：

a、拜访网络内的业务服务器直接向本网络内 AAA 服务器发送查询该 TID 所对应的用户是否合法的消息，

b、接收到步骤 a 所述查询消息的 AAA 服务器根据该消息中的 TID 确认该用户所属归属网络后，直接向该漫游用户所属归属网络内的 AAA 服务器发送查询该 TID 所对应的用户是否合法的消息；

c、归属网络内的 AAA 服务器直接向本网络中的 BSF 进行查询，BSF 在本地检测到与该 TID 对应的用户信息后，通过本网络中的 AAA 服务器和拜访网络中的 AAA 服务器给拜访网络中的业务服务器返回与该 TID 对应的用户信息；

d、拜访网络内的业务服务器接收到来自本网络的 AAA 服务器的与该 TID 对应的用户信息后，建立与该漫游用户之间的信任关系。

5、根据权利要求 2 或 4 所述的方法，其特征在于，所述与该 TID 对应的用户信息至少包括密钥信息和用户的身份标识。

6、根据权利要求 5 所述的方法，其特征在于，所述与该 TID 对应的用户信息还包括与安全相关的 profile 信息。

7、根据权利要求 1 所述的方法，其特征在于，所述根据该漫游用户所属归属网络的通用鉴权框架的鉴权结果，建立拜访网络业务内服务器和漫游用户之间的信任关系进一步包括以下步骤：

a、拜访网络内的业务服务器通知漫游用户该标识非法，并提示用户使用永久身份标识；

b、拜访网络内的业务服务器再次接收到来自漫游用户的包含永久身份标识的业务请求信息后，向本网络内的 AAA 服务器发出鉴权请求；拜访网络内的 AAA 服务器根据用户的永久身份标识确认出该用户所属的归属网络后，直接向该漫游用户所属归属网络内的 AAA 服务器发送对该用户进行鉴权的请求；

c、归属网络内的 AAA 服务器接收到来自拜访网络 AAA 服务器的鉴权请求后，请求本网络内的 BSF 对该用户进行鉴权；

d、归属网络内的 BSF，经本网络内的 AAA 服务器、拜访网络内的 AAA 服务器以及拜访网络内的 BM-SC，与用户进行 AKA 鉴权，鉴权成功后，直接给拜访网络内的 BM-SC 返回鉴权成功消息，且该消息中包含对该用户的授权

信息；

e、拜访网络内的业务服务器接收到归属网络内的 AAA 服务器和本网络内的 AAA 服务器转发的用户授权信息，建立与该漫游用户之间的信任关系。

8、根据权利要求 7 所述的方法，其特征在于，所述用户的授权信息中至少包括：密钥信息和和用户的身份标识。

9、根据权利要求 8 所述的方法，其特征在于，所述用户的身份标识的类型根据网络运营商的策略而定。

10、根据权利要求 1 所述的方法，其特征在于，该方法进一步包括：漫游用户与所属归属网络内的 BSF 进行了成功的 AKA 鉴权，向拜访网络内的业务服务器发送包含 TID 标识的业务请求消息，然后再执行后续步骤。

说　明　书

一种实现漫游用户使用拜访网络内业务的方法

技术领域

本发明涉及第三代无线通信技术领域，特别是指一种实现漫游用户使用拜访网络内业务的方法。

背景技术

在第三代无线通信标准中，通用鉴权框架是多种应用业务实体使用的一个用于完成对用户身份进行验证的通用结构，应用通用鉴权框架可实现对应用业务的用户进行检查和验证身份。上述多种应用业务可以是多播/广播业务、用户证书业务、信息即时提供业务等，也可以是代理业务，例如多个服务和一个代理相连，通用鉴权框架把代理也当作一种业务来处理，组织结构可以很灵活，而且，对于以后新开发的业务也同样可以应用通用鉴权框架对应用业务的用户进行检查和验证身份。

图 1 所示为通用鉴权框架的结构示意图。通用鉴权框架通常由用户 101、执行用户身份初始检查验证的实体（BSF）102、用户归属网络服务器（HSS）103 和网络应用实体（NAF）104 组成。BSF 102 用于与用户 101 进行互验证身份，同时生成 BSF 102 与用户 101 的共享密钥；HSS 103 中存储用于描述用户信息的描述（Profile）文件，同时 HSS 103 还兼有产生鉴权信息的功能。

用户需要使用某种业务时，如果其知道该业务需要到 BSF 进行互鉴权过程，则直接到 BSF 进行互鉴权，否则，用户会首先和该业务对应的 NAF 联系，如果该 NAF 使用通用鉴权框架，并且发现发出请求的用户还未到 BSF 进行互认证过程，则通知发出请求的用户到 BSF 进行身份验证。

用户与 BSF 之间的互认证过程是：BSF 接到来自用户的鉴权请求后，

首先到 HSS 获取该用户的鉴权信息，根据所获取的鉴权信息与用户之间执行鉴权和密钥协商协议（AKA）进行互鉴权。认证成功后，用户和 BSF 之间互相认证了身份并且同时生成了共享密钥 Ks。之后，BSF 分配一个会话事务标识（TID）给用户，该 TID 是与 Ks 相关联的。

用户收到这个 TID 后，重新向 NAF 发出连接请求，且请求消息中携带了该 TID。NAF 收到请求后，先在本地查询是否有用户携带的该 TID，如果 NAF 不能在本地查询到该 TID，则向 BSF 进行查询。BSF 查询到该 TID 后，将该 TID 以及该 TID 对应密钥信息包含在发送给 NAF 的成功响应消息中。NAF 收到来自 BSF 的成功响应消息后，即认为该用户是经过 BSF 认证的合法用户，同时 NAF 和用户也共享了密钥 Ks 或由 Ks 衍生的密钥。此时，NAF 与该用户在密钥 Ks 或由 Ks 衍生的密钥的保护下进行正常的通信。如果 BSF 不能在本地查询到该 TID，则通知 NAF 没有该用户的信息，此时，NAF 将通知用户到 BSF 进行认证鉴权。

下面以多播/广播业务（MBMS）为例，具体说明通用鉴权框架的用法。在无线通信领域中，多播业务是一种一点到多点的单向承载业务，数据是由一个源实体，传送到多个接收实体。在某一区域内的已订阅多播业务的用户，能够接收多播业务的服务。在多播业务中需要防止没有订阅或未付费的用户享受多播业务，因此在多播业务的群组中，针对某个具体业务都设置一个多播服务密钥（MSK）密钥，MSK 只有群组内的用户和提供多播的业务的服务器知道，而群组外的用户无权知道这个密钥。多播业务服务器使用多播业务密钥（MTK）对业务数据信息进行加密，群组内的用户收到业务数据信息后使用相同的共享多播业务密钥 MTK 解密，从而获得业务数据信息的内容，而群组外用户因为没有这个共享密钥，所以不能获取多播信息内容。共享的 MSK 并不直接加密该 MBMS 业务的数据，它用来做接入控制，产生 MTK 或对 MTK 进行加密。

用户应用 MBMS 时，首先要经过通用鉴权框架的鉴权，即应用通用鉴

权框架中的 BSF 代替 MBMS 的服务器对用户进行鉴权，而 MBMS 中的多播/广播服务器（BM-SC）则相当于通用鉴权框架中的 NAF。BSF 对用户进行鉴权后，BSF 与用户了共享密钥 Ks,并且 BSF 给该用户分配了 TID，然后用户使用 TID 向 BM-SC 发出业务请求，BM-SC 收到用户包含 TID 的请求后，向 BSF 进行查询，BSF 查到该用户的信息后，返回密钥 Ks 或 Ks 衍生的密钥。这样 BM-SC 与用户也就共享了密钥 Ks 或由 Ks 衍生的密钥，该密钥为 MBMS 业务中的多播用户密钥（MUK），用来保护 BM-SC 到用户之间点到点的群组共享密钥 MSK。也就是说，此时，用户与 BM-SC 之间建立了信任关系（security association），即用户相信它所连接的服务器是真实而且合法的服务器，而不是由其它设备假冒的服务器，同时业务服务器也相信请求业务的用户是一个合法用户，而不是一个攻击者。

在现有技术中，通用鉴权框架只考虑了在本网络中的使用问题，没有考虑如何使处于漫游状态的用户使用其归属网络中的通用鉴权框架。

在实际应用中，应用通用鉴权框架进行鉴权的用户处于漫游状态时，通常需要使用拜访网络的某些业务，例如漫游用户需要了解当地新闻、天气、交通等信息。由于现有技术没有考虑在拜访网络中如何使用归属网络的通用鉴权框架，因此将导致漫游的通用鉴权框架用户不能应用通用鉴权框架与拜访网络的业务服务器建立信任关系，从而使得漫游的通用鉴权框架用户不能使用拜访网络中的业务。

发明内容

有鉴于此，本发明的目的在于提供一种实现漫游用户使用拜访网络内业务的方法，使漫游用户和拜访网络的业务服务器能够通过该用户所属归属网络内的通用鉴权框架建立信任关系，从而能够正常使用拜访网络提供的业务。

为达到上述目的，本发明的技术方案是这样实现的：

一种实现漫游用户使用拜访网络内业务的方法，该方法包括以下步骤：

拜访网络内的业务服务器接收到来自漫游用户的包含TID信息的业务请求消息后，根据该漫游用户所属归属网络的通用鉴权框架鉴权结果，建立拜访网络内业务服务器和漫游用户之间的信任关系，实现漫游用户使用拜访网络内业务。

较佳地，所述根据该漫游用户所属归属网络的通用鉴权框架的鉴权结果，建立拜访网络业务内服务器和漫游用户之间的信任关系进一步包括以下步骤：

a、拜访网络内的业务服务器直接向本网络内的 BSF 或通用鉴权框架代理发送查询该 TID 所对应的用户是否合法的消息；

b、接收到步骤 a 所述查询消息的 BSF 或通用鉴权框架代理，直接向归属网络内的 BSF 发送查询与该 TID 所对应的用户是否合法的消息；

c、归属网络内的 BSF 在本地检测到与该 TID 对应的用户信息后，给拜访网络内的 BSF 或通用鉴权框架代理返回与该 TID 对应的用户信息；

d、拜访网络内的业务服务器接收到本网络内的 BSF 或通用鉴权框架代理返回的与该 TID 对应的用户信息后，建立与该漫游用户之间的信任关系。

较佳地，所述通用鉴权框架代理是一个独立的服务器，或与本网络内的 AAA 服务器合设的服务器，或与本网络内的业务服务器合设的服务器。

较佳地，所述根据该漫游用户所属归属网络的通用鉴权框架的鉴权结果，建立拜访网络内业务服务器和漫游用户之间的信任关系进一步包括以下步骤：

a、拜访网络内的业务服务器直接向本网络内 AAA 服务器发送查询该 TID 所对应的用户是否合法的消息，

b、接收到步骤 a 所述查询消息的 AAA 服务器根据该消息中的 TID 确认该用户所属归属网络后，直接向该漫游用户所属归属网络内的 AAA 服务器发送查询该 TID 所对应的用户是否合法的消息；

c、归属网络内的 AAA 服务器直接向本网络中的 BSF 进行查询，BSF 在本地检测到与该 TID 对应的用户信息后，通过本网络中的 AAA 服务器和拜访网络中的 AAA 服务器给拜访网络中的业务服务器返回与该 TID 对应的用户信息；

d、拜访网络内的业务服务器接收到来自本网络的 AAA 服务器的与该 TID 对应的用户信息后，建立与该漫游用户之间的信任关系。

较佳地，所述与该 TID 对应的用户信息至少包括密钥信息和用户的身份标识。

较佳地，所述与该 TID 对应的用户信息还包括与安全相关的 profile 信息。

较佳地，所述根据该漫游用户所属归属网络的通用鉴权框架的鉴权结果，建立拜访网络业务内服务器和漫游用户之间的信任关系进一步包括以下步骤：

a、拜访网络内的业务服务器通知漫游用户该标识非法，并提示用户使用永久身份标识；

b、拜访网络内的业务服务器再次接收到来自漫游用户的包含永久身份标识的业务请求信息后，向本网络内的 AAA 服务器发出鉴权请求；拜访网络内的 AAA 服务器根据用户的永久身份标识确认出该用户所属的归属网络后，直接向该漫游用户所属归属网络内的 AAA 服务器发送对该用户进行鉴权的请求；

c、归属网络内的 AAA 服务器接收到来自拜访网络 AAA 服务器的鉴权请求后，请求本网络内的 BSF 对该用户进行鉴权；

d、归属网络内的 BSF，经本网络内的 AAA 服务器、拜访网络内的 AAA 服务器以及拜访网络内的 BM-SC，与用户进行 AKA 鉴权，鉴权成功后，直接给拜访网络内的 BM-SC 返回鉴权成功消息，且该消息中包含对该用户的授权信息；

e、拜访网络内的业务服务器接收到归属网络内的 AAA 服务器和本网络内的 AAA 服务器转发的用户授权信息，建立与该漫游用户之间的信任关系。

较佳地，所述用户的授权信息中至少包括：密钥信息和和用户的身份标识。

较佳地，所述用户的身份标识的类型根据网络运营商的策略而定。

较佳地，该方法进一步包括：漫游用户与所属归属网络内的 BSF 进行了成功的 AKA 鉴权，向拜访网络内的业务服务器发送包含 TID 标识的业务请求消息，然后再执行后续步骤。

应用本发明，当拜访网络内的业务服务器接收到来自漫游用户的包含TID信息的业务请求消息后，根据该漫游用户所属归属网络的通用鉴权框架鉴权结果，建立拜访网络业务服务器和漫游用户之间的信任关系，从而实现了漫游用户通过该用户所属归属网络内的通用鉴权框架使用拜访网络内的业务。由于本发明使得漫游用户在使用拜访网络业务时，仍然可以使用本网通用鉴权框架的鉴权结果，因而充分利用了现有网络结构，节省了资源。本发明增加了一种用户使用拜访网络业务的途径，使得拜访网络能够最大限度的为用户提供业务。另外，即使拜访网络内的业务服务器完全不认识TID标识，漫游用户也可以应用其所属网络的通用鉴权框架完成鉴权过程，从而减少了由AAA服务器进行鉴权时因序列号（SQN）失步造成的鉴权失败的情况。

附图说明

图1所示为通用鉴权框架的结构示意图；

图2所示为应用本发明实施例一的示意图；

图3所示为应用本发明实施例二的示意图；

图4所示为应用本发明实施例三的示意图。

具体实施方式

为使本发明的技术方案更加清楚，下面结合附图及具体实施例再对本发明做进一步地详细说明。

本发明的思路是：拜访网络中的业务服务器接收到来自漫游用户的业务请求后，通过本网络的BSF，或本网络的通用鉴权框架代理，或本网络内的AAA服务器以及该漫游用户所属归属网络内的AAA服务器，利用归属网络的通用鉴权框架的鉴权结果，建立拜访网络业务服务器和漫游用户之间的信任关系；从而实现了漫游用户经过归属网络内的通用鉴权框架鉴权后使用其所在拜访网络内的业务。

为了更好地说明漫游用户如何使用归属网络中的通用鉴权框架，下面首先说明几种可能存在的情况。

对于漫游用户而言，其可能需要使用归属网络中的业务，也可能需要使用拜访网络中的业务。

当漫游用户使用归属网络中的业务时，由于网络间都是 IP 连接，因而漫游用户可通过应用层直接与归属网络中的业务服务器进行通信，并可以直接使用归属网络中的通用鉴权框架。这与现有技术使用方法完全相同。

下面具体说明漫游用户使用拜访网络内业务的情况。

对于漫游用户所在的拜访网络而言，其可能存在以下四种情况：

1）该用户所在的拜访网络支持通用鉴权框架。

2）该用户所在的拜访网络不支持通用鉴权框架，但支持通用鉴权框架代理。在这种情况下，拜访网络内可能存在一个单独的支持通用鉴权框架代理的服务器，但在实际应用中，通常将该服务器与其它实体合设，例如将支持通用鉴权框架代理的服务器与 AAA 合设，由 AAA 实现支持通用鉴权框架代理的功能，即由 AAA 实现对 TID 分析和路由功能；拜访网络内也可能不存在支持通用鉴权框架代理的单独的服务器，而是拜访网络中的各个服务器均支持通用鉴权框架代理功能，即由每个实际的业务服务器实现对 TID 分析和路由功能（由于 1）和 2）的处理方法很类似，在下面以一个实施例加以说明）。

3）该用户所在的拜访网络不支持通用鉴权框架，也不支持通用鉴权框架代理，且拜访网络中的业务服务器不对 TID 进行鉴别，也不对 TID 进行处理，仅把 TID 标识看作是一种用户身份标识，并将该标识直接传递给本网络中的 AAA 服务器，请求 AAA 服务器进行鉴权。

4）该用户所在的拜访网络不支持通用鉴权框架，也不支持通用鉴权框架代理，且拜访网络中的业务服务器对自身接收到的标识进行鉴别，但由于在拜访网络中根本没有通用鉴权框架的概念，所以业务服务器不认识 TID 标

识，因此它要求用户使用自己的永久身份标识，如国际移动用户识别码（IMSI）等。

下面以漫游用户应用其所在拜访网络中的 MBMS 业务为例，具体说明其实现应用拜访网络内业务的方法，其中 BM-SC 为 MBMS 业务的业务服务器。

图 2 所示为应用本发明实施例一的示意图。业务服务器通过直接查询该漫游用户在所属归属网络的通用鉴权框架鉴权结果，与漫游用户之间建立信任关系的步骤如下：

步骤 201，漫游用户与归属网络内通用鉴权框架中的 BSF 执行 AKA 互鉴权，鉴权通过后，得到了 BSF 分配的 TID，且此时漫游用户与归属网络内的 BSF 共享了密钥 Ks；

步骤 202，漫游用户向拜访网络的 BM-SC 发送包含 TID 信息的业务请求消息；

步骤 203，如果拜访网络支持通用鉴权框架，则 BM-SC 向本网络内的 BSF 发送查询与该 TID 相对应的用户信息，以判断该用户是否通过鉴权，即判断该用户是否合法；

如果拜访网络仅支持通用鉴权框架代理功能，且支持通用鉴权框架代理功能由一个单独的服务器实现，该则 BM-SC 向本网络内实现通用鉴权框架代理的服务器发送查询与该 TID 对应的用户信息；

如果拜访网络仅支持通用鉴权框架代理，且是每个业务服务器自己支持通用鉴权框架代理的功能，则 BM-SC 同样查询与该 TID 对应的用户信息，只是该查询是在该业务服务器的内部接口中实现；

步骤 204，拜访网络内的 BSF 或通用鉴权框架代理，根据接收到的 TID 标识判断该漫游用户所属的归属网络；

步骤 205，拜访网络内的 BSF 或通用鉴权框架代理向漫游用户所属归属网络内的 BSF 查询与该 TID 对应的用户信息，即查询该用户是否合法；

步骤 206，归属网络的 BSF 检索到与该 TID 对应的用户信息后，根据本地运营商的策略进行处理，该处理可以是直接发送与 TID 对应的密钥 Ks 给请求者，或对密钥 Ks 进行密钥衍生，将衍生的密钥发送给请求者，同时设定所发送密钥的有效期限；

步骤 207，归属网络的 BSF 返回与与该 TID 对应的用户信息给拜访网络的 BSF 或通用鉴权框架代理；上述与该 TID 对应的用户信息包括密钥信息、用户的身份标识，和与安全相关的 profile 信息，其中，密钥信息和用户的身份标识是必选项，密钥信息用于保证用户与 BM-SC 之间进行正常的通信，用户的身份标识用于计费，如果拜访网络不能确定用户的真实身份，在其与归属网络进行网间结算时将出现问题；与安全相关的 profile 信息是可选项；

步骤 208，拜访网络的 BSF 或通用鉴权框架代理将 TID 的相关信息返回给 BM-SC，BM-SC 收到与该 TID 对应的用户信息后，即建立了与漫游用户之间的信任关系，也就是认为该请求用户合法，同时，BM-SC 也和 UE 共享了 Ks 或由 Ks 衍生的密钥，该密钥作为 MBMS 业务的 MUK，用于保护群组共享密钥 MSK 的点到点保密传送；

步骤 209，BM-SC 发确认消息给该用户，并和该用户进行 MBMS 业务内部密钥分发，业务发送等相关的业务过程。

至此，漫游用户实现了使用归属网络中的通用鉴权框架应用拜访网络中的业务。上述方法适用于漫游用户所在拜访网络支持通用鉴权框架，或支持通用鉴权框架代理的情况。

图 3 所示为应用本发明实施例二的示意图。业务服务器通过直接查询该漫游用户在所属归属网络的通用鉴权框架鉴权结果，与漫游用户之间建立信任关系的步骤如下：

步骤 301，漫游用户与归属网络内通用鉴权框架中的 BSF 执行 AKA 互鉴权，鉴权通过后，得到了 BSF 分配的 TID，且此时漫游用户与归属网络内的 BSF 共享了密钥 Ks；

步骤 302，漫游用户向拜访网络的 BM-SC 发送包含 TID 信息的业务请求消息；

步骤 303，拜访网络的 BM-SC 不检查该用户的身份是否合法，而是直接将该 TID 作为用户身份标识，向本网络内的 AAA 服务器发出查询请求，即请求本网络的 AAA 对该用户进行鉴权，即判断该用户是否合法；

步骤 304，拜访网络的 AAA 服务器根据 TID 标识的格式（TID 的标识格式为用户标识@域名），判断出用户所属的归属网络；

步骤 305，拜访网络的 AAA 服务器向该漫游用户所属归属网络内的 AAA 服务器发出查询 TID 的请求，即请求归属网络内的 AAA 服务器对该用户进行鉴权；

步骤 306，归属网络内的 AAA 服务器收到查询 TID 的消息后，由于其知道 TID 标识是由本网的通用鉴权框架中的 BSF 分配的，因此其向 BSF 进行查询；BSF 和 AAA 服务器在某些执行功能上是类似的，所以 BSF 也可能是由网络中的某个 AAA 服务器来兼任，在这种情况下，BSF 和 AAA 服务器之间的消息是内部接口消息；

步骤 307，归属网络的 BSF 检索到与该 TID 对应的用户信息后，根据本地运营商的策略进行处理，该处理可以是直接发送与 TID 对应的密钥 Ks 给请求者，或对密钥 Ks 进行密钥衍生，将衍生的密钥发送给请求者，同时设定所发送密钥的有效期限；

步骤 308，归属网络的 BSF 返回与与该 TID 对应的用户信息给本网络的 AAA 服务器；上述与该 TID 对应的用户信息包括密钥信息、用户的身份标识，和与安全相关的 profile 信息，其中，密钥信息和用户的身份标识是必选项，密钥信息用于保证用户与 BM-SC 之间进行正常的通信，用户的身份标识用于计费，如果拜访网络不能确定用户的真实身份，在其与归属网络进行网间结算时将出现问题；安全相关的 profile 信息是可选项；

步骤 309，归属网络的 AAA 服务器返回与与该 TID 对应的用户信息给

拜访网络内的 AAA 服务器；拜访网络内的 AAA 服务器接收到归属网络的 AAA 服务器返回的消息后，即认为归属网络已经对用户进行了鉴权，该查询返回消息相当于授权消息；

步骤 310，拜访网络的 AAA 服务器将与该 TID 对应的用户信息返回给 BM-SC，BM-SC 收到 TID 相关信息后，即建立了与漫游用户之间的信任关系，也就是认为该请求用户合法，同时，BM-SC 也和 UE 共享了 Ks 或由 Ks 衍生的密钥，该密钥作为 MBMS 业务的 MUK，用于保护群组共享密钥 MSK 的点到点保密传送；

步骤 311，BM-SC 发确认消息给该用户，并和该用户进行 MBMS 业务内部密钥分发，业务发送等相关的业务过程。

至此，漫游用户实现了使用归属网络中的通用鉴权框架应用拜访网络中的业务。上述方法适用于漫游用户所在拜访网络不支持通用鉴权框架，也不支持通用鉴权框架代理，且拜访网络中的业务服务器不鉴别 TID 标识，只是将其作为一种用户身份标识，传递给本网络中的 AAA 服务器，请求 AAA 服务器对该用户进行鉴权的情况。

图 4 所示为应用本发明实施例三的示意图。业务服务器通过与该漫游用户所属归属网络的通用鉴权框架实施鉴权过程，获取鉴权结果，根据该鉴权结果与漫游用户之间建立信任关系的步骤如下：

步骤 401，漫游用户与归属网络内通用鉴权框架中的 BSF 执行 AKA 互鉴权，鉴权通过后，得到了 BSF 分配的 TID，且此时漫游用户与归属网络内的 BSF 共享了密钥 Ks；

步骤 402，漫游用户向拜访网络的 BM-SC 发送包含 TID 信息的业务请求消息；

步骤 403，由于 BM-SC 不能识别 TID 标识，因此 BM-SC 通知漫游用户该标识非法，并提示用户使用永久身份标识，如 IMSI 等；

步骤 404，漫游用户向 BM-SC 发送包含永久身份标识的业务请求；

步骤405，拜访网络的BM-SC向本网络内的AAA服务器发出鉴权请求；

步骤406，拜访网络的AAA服务器根据用户的身份标识判断出用户的归属网络，然后向该漫游用户所属归属网络内的AAA服务器发出鉴权请求；

步骤407，归属网络内的AAA服务器请求本网络内的通用鉴权框架中的BSF进行鉴权，这是因为：虽然AAA服务器本身具有鉴权计费功能，且在地位上是与BSF相同的，但在实际应用中，不同的AAA服务器在对用户进行鉴权时，容易出现因序列号（SQN）失步而导致鉴权失败的情况，出现的具体原因在现有已公布的文章中有描述，所以对通用鉴权框架支持的业务采用通用鉴权框架对用户进行鉴权，以保证鉴权的成功率；

步骤408，归属网络内BSF与用户完成AKA的鉴权过程，该鉴权过程中的消息在逻辑上是经过拜访网络的BM-SC，拜访网络的AAA，归属网络的AAA转发的；

步骤409，鉴权成功后，归属网络内的BSF给拜访网络的BM-SC返回鉴权成功消息，因为归属网络内的BSF已经知道鉴权请求是来自哪个具体的业务服务器，因此，归属网络内的BSF直接将用户的密钥资料等信息包含在鉴权成功和授权的消息中，如果归属网络内的BSF在鉴权的同时给用户分配了TID，则该TID也可以包括在授权消息中通知给BM-SC服务器；

步骤410，归属网络内的AAA服务器向拜访网络内的AAA服务器转发该鉴权成功的消息；

步骤411，拜访网络的AAA服务器转发鉴权成功和授权消息给BM-SC，即BM-SC建立了与漫游用户之间的信任关系；虽然BM-SC不能够识别TID标识，但它仍然可以在后面的通信中使用TID，这时TID将作为一种临时身份标识使用，其使用的方法与现有临时身份标识的使用方法相同；

步骤412，BM-SC收到鉴权成功和授权消息后，发确认消息给该用户，并和该用户进行MBMS业务内部密钥分发，业务发送等相关的业务过程。至于BM-SC和用户在后续的通信过程中使用哪种用户身份标识，根据拜访

网络运营商的策略而定。

至此，漫游用户实现了使用归属网络中的通用鉴权框架应用拜访网络中的业务。上述方法适用于该用户所在的拜访网络不支持通用鉴权框架，也不支持通用鉴权框架代理，且拜访网络中的业务服务器对用户请求消息中的标识进行鉴别，但因为在拜访网络中根本没有通用鉴权框架的概念，所以业务服务器不能识别 TID 标识，因此业务服务器要求用户使用自己的永久身份标识的情况。

以上所述仅为本发明的较佳实施例而已，并不用以限制本发明，凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

说 明 书 附 图

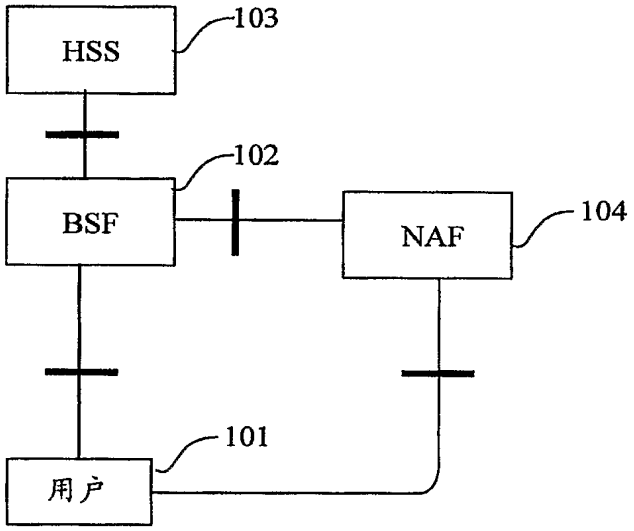

HSS
103
BSF
102
NAF
104
用户
101

图 1

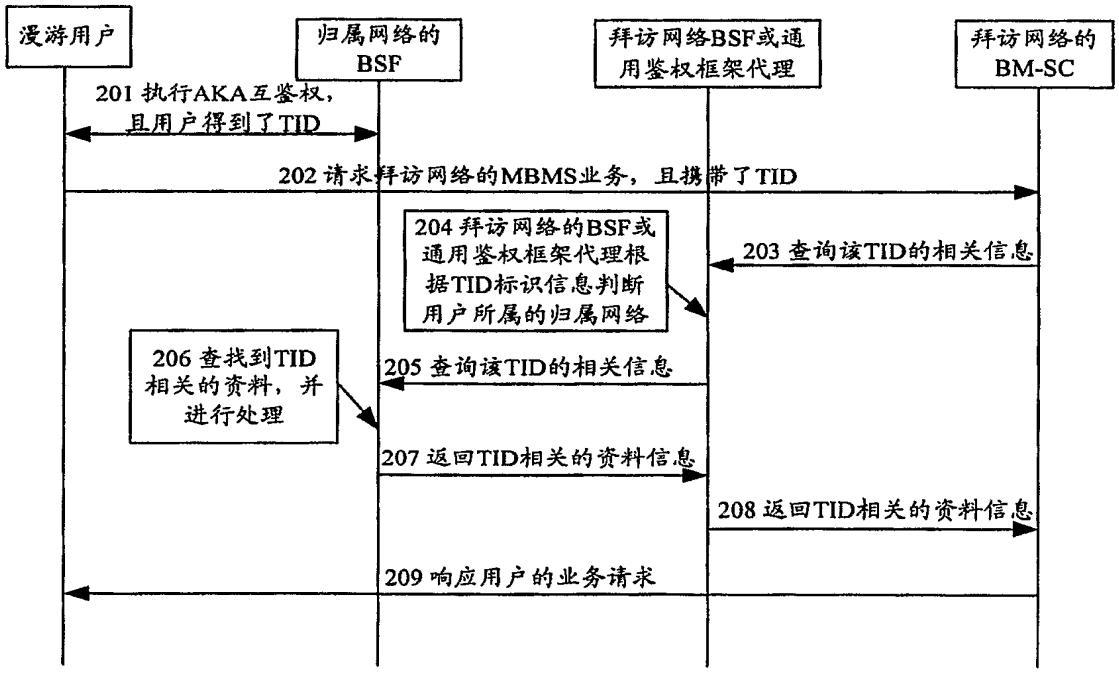

浸游用户
归属网络的BSF
拜访网络BSF或通用鉴权框架代理
拜访网络的BM-SC
201 执行AKA互鉴权，且用户得到了TID
202 请求拜访网络的MBMS业务，且携带了TID
204 拜访网络的BSF或通用鉴权框架代理根据TID标识信息判断用户所属的归属网络
203 查询该TID的相关信息
206 查找到TID相关的资料，并进行处理
205 查询该TID的相关信息
207 返回TID相关的资料信息
208 返回TID相关的资料信息
209 响应用户的业务请求

图 2

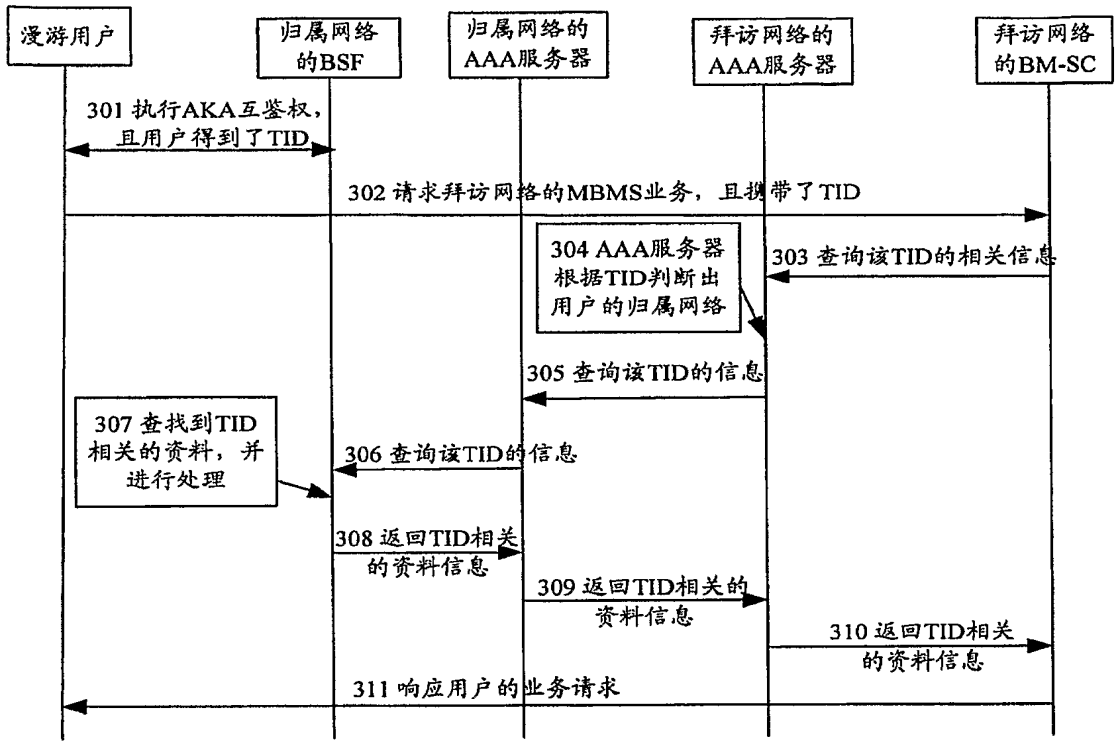

漫游用户
归属网络的BSF
归属网络的AAA服务器
拜访网络的AAA服务器
拜访网络的BM-SC
301 执行AKA互鉴权，且用户得到了TID
302 请求拜访网络的MBMS业务，且携带了TID
304 AAA服务器根据TID判断出用户的归属网络
303 查询该TID的相关信息
305 查询该TID的信息
307 查找到TID相关的资料，并进行处理
306 查询该TID的信息
308 返回TID相关的资料信息
309 返回TID相关的资料信息
310 返回TID相关的资料信息
311 响应用户的业务请求

图 3

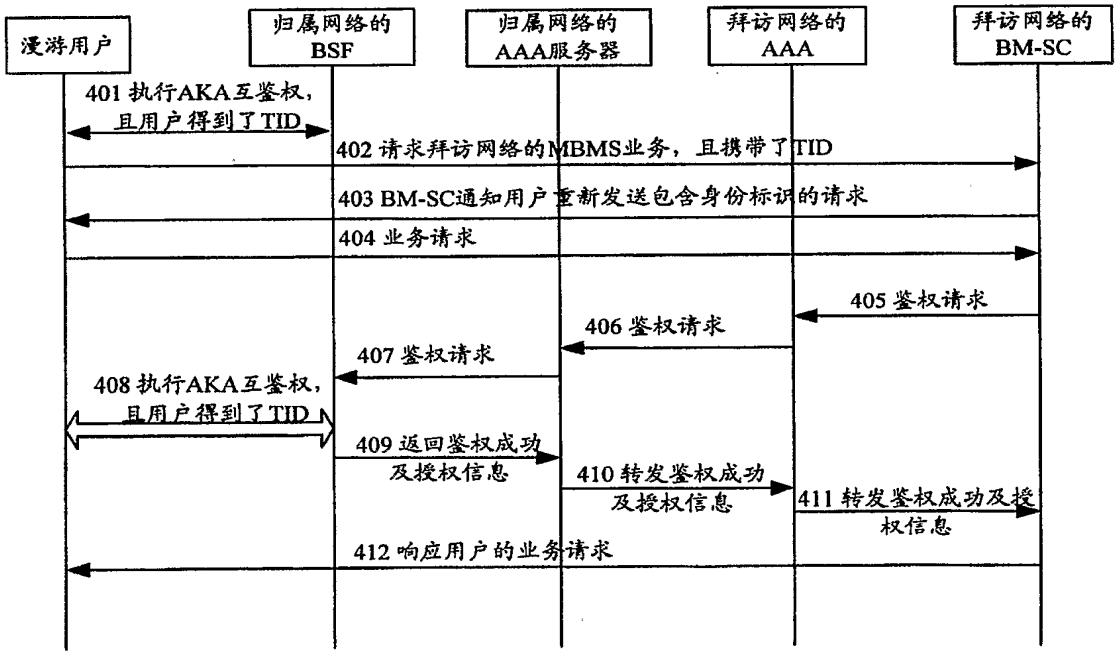

漫游用户
归属网络的BSF
归属网络的AAA服务器
拜访网络的AAA
拜访网络的BM-SC
401 执行AKA互鉴权，且用户得到了TID
402 请求拜访网络的MBMS业务，且携带了TID
403 BM-SC通知用户重新发送包含身份标识的请求
404 业务请求
405 鉴权请求
406 鉴权请求
407 鉴权请求
408 执行AKA互鉴权，且用户得到了TID
409 返回鉴权成功及授权信息
410 转发鉴权成功及授权信息
411 转发鉴权成功及授权信息
412 响应用户的业务请求

图 4